Upholding information rights

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

The Information Commissioner's response to the Department of Finance's consultation on the NI Open Data Strategy Review

Introduction

1. The Information Commissioner (the Commissioner) is pleased to respond to the Department of Finance's (DoF) consultation on the Northern Ireland (NI) Open Data Strategy Review.

2. The Commissioner has responsibility for promoting and enforcing the EU General Data Protection Regulation (GDPR), the UK Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations, as well as the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. She also deals with complaints under the Re-use of Public Sector Information Regulations 2015 (RPSI) and the INSPIRE Regulations 2009.

3. The Commissioner is independent of government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

4. Open data initiatives seek to increase the proactive publication of information by public bodies as well as improving ease of access and enhancing the re-use of information by the use of standardised, open formats. However, it is vital that open data complies with legislation, including recent changes to data protection law. It is also important that these initiatives take into consideration other information rights legislation which are often complementary to this agenda.

5. The Commissioner welcomes the refreshing of an open data strategy and recognises there may be economic benefits to consumers, businesses and other organisations arising from the publication of open data sets.

General observations

6. It would be useful to put into context the timeframe of the existing Open Data Strategy for NI i.e. 2015-2018. The Data Protection Act 1998 was in force for the duration of most of this period. A refreshed Open Data Strategy for NI should make explicit reference to the GDPR and Data Protection Act (2018) which are the applicable data protection laws during any proposed strategy period. This consultation response will be reflective of this newly introduced legislation.

7. It may be helpful in a revised Open Data Strategy to make reference from the outset to other information rights legislation (e.g. FOIA, EIR, PECR, INSPIRE and RPSI) which may influence the course of decisions about certain types of data to be made open. It could be recommended that any questions about data protection legislation, including what data should be made open, should be raised with the organisation's DPO. Part of the role of the DPO under the GDPR is to advise and inform their organisation of their obligations under data protection law. They must be involved from the outset in all issues relating to data protection. Other questions about datasets could also be raised with the information governance staff in terms of obligations and exemptions under the other information rights legislation.

8. The Commissioner would welcome the inclusion of a focus on protecting privacy and considers that this would be helpful reference in a refreshed strategy. As per the concept of 'Data Protection by Design and Default' under Article 25 of GDPR, DoF and other Departments or bodies participating in the open data work could consider adopting this ethos into any proposals for future processing. Implementing technical and organisational measures, at the earliest stages of the design of their processing operation, could lead to the safeguarding of privacy and data protection principles from the start. The refreshed strategy should make reference to the potential risk of disclosing personal data and the benefits of taking the above mentioned approach.

9. The Commissioner welcomes the focus on transparency in the current Open Data Strategy 2015-2018. Transparency and accountability are important elements of building trust and confidence in the Government's use of data but transparency and clarity for individuals is also very important. The GDPR requires enhanced transparency and accountability by organisations in order to achieve compliance. It is worth noting that the ICO is currently consulting on a draft access to information strategy entitled, 'Openness by Design. Our Draft access to information strategy.' One of the key priorities proposed is

to work in partnership to improve standards of openness, transparency and participation among public authorities in a digital age. Given this, the Commissioner believes that the refresh of the open data strategy offers a timely opportunity to build upon this focus on transparency and openness. It also can allow for any ensuing strategy and implementation plan to enhance current information management practices and to support an 'open by default' culture.

Definitions of Personal Data and other terminology

Personal Data

10. A refreshed strategy with updated proposals will undoubtedly make reference to various types of data. The existing strategy did not define the range and categories of data that may or may not be captured in open data initiatives. It is the Commissioner's view that there may be advantages in defining the terminology in the strategy from the outset, with that used in the GDPR; otherwise there is the risk that practitioners in individual departments may be confused about whether certain information they are making open is personal data.

11. The Commissioner will not express a view on the approach taken by the Departments on what types of data will be used in the open data process, but the decision on what is and what is not personal data is a basic one that we would expect the data provider to be aware of. It may be helpful to include the definition of personal data which can be found under Article 4 of the GDPR[1]. It is also included in the annex to this response. The Commissioner's current guidance on 'what is personal data' will be useful in this regard.

Anonymisation

12. The Commissioner believes that it may be useful to define what is meant by anonymised data throughout the strategy in order to ensure that there is a common understanding of what data will be suitable to become 'open'.

13. Recital 26 of the GDPR describes what is meant by anonymised data and how it can be deemed as outside of the scope of data protection law: "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to

[1] 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

an identified or identifiable natural person or to personal data rendered anonymous in such a way that the data subject is not or no longer identifiable." Wider reference to this concept will be made throughout the course of this response.

Pseudonymisation

14. The Commissioner believes that the concept of pseudonymisation should be defined throughout the refreshed strategy. This will ensure that there is no confusion amongst data controllers and that they have in fact rendered their data suitable for inclusion within the scope of open data. Pseudonymisation is defined within the GDPR Article 4 (3)(b) as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified of identifiable individual." The Commissioner will make further reference to this concept through this response.

Nine Open Data Principles

15. The nine open data principles do not state what data should be public and open, nor are they intended to. But rather, the principles specify the conditions that data should meet to be considered open. The Commissioner believes that principles can provide the framework for a successful open data agenda. Article 5 of the GDPR sets out seven key principles which lie at the heart of the data protection regime. Compliance with the spirit of these principles is therefore a fundamental building block for good data protection practice. Likewise, the success of the new open data regime will be achieved by compliance with the open data principles. Therefore it will be important to set them out at the start of the revised strategy as they should inform everything else that follows.

16. To further enhance the success of the new strategy, the Commissioner recommends that the current open data principles are reviewed to ensure they fit with the evolving information rights landscape.

Transparency about reasons for withholding datasets

17. The Commissioner welcomes the reference on page 15 of the existing strategy to transparency about reasons why data cannot be released. A refreshed strategy could elaborate on this further to encourage openness and aid understanding of the factors that will influence a decision to release a dataset.

Contracts

18. The Commissioner notes the intention in the existing strategy that open standards for publishing data will be built into contracts and procurements for services and systems. The Commissioner's experience of dealing with complaints about public authorities' handling of FOIA requests shows that there is some uncertainty as to whether certain information held by contractors is in effect held on behalf of the public authority, (and hence potentially accessible under FOIA) or whether it is the company's own information, and hence out of scope of FOIA. Our report on outsourcing (referred to in paragraphs 43 and 44 below) covers many of these issues and due consideration should be given to its content.

RPSI

19. The Commissioner believes that it may be important to make reference to the Re-use of Public Sector Information Regulations 2015 (RPSI). The ICO deals with complaints about how public sector bodies have dealt with requests to re-use information. It may also be helpful to point out that RPSI does not apply to information that would be exempt from disclosure under information access legislation. For further information please see our guide to RPSI.

Data security and risk

20. Section 7 on Risks in the current DoF strategy, mentions how anonymising and aggregating data properly can mean that personal data is not disclosed. This point, although very important, is not the only risk to consider in terms of open data and data protection. We believe a refreshed strategy should make particular reference to personal data breaches.

21. The GDPR defines personal data breaches as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data*". Under the GDPR, personal data breaches which are likely to result in a risk to the rights and freedoms of individuals, must be reported to the ICO within 72 hours of the controller becoming aware of it and confirming it represents a breach. This should be clear in the strategy when describing risk.

22. It may also be helpful to reflect in the strategy the breadth of instances which can constitute a breach through the provision of open data. For example, linked to paragraph 11 on defining personal data, it is imperative that the data provider is in fact aware of what personal data he or she holds. If it is unclear, this could inadvertently become included in data which is made 'open.'

23. The Strategy could signpost to the Commissioner's guidance on data breach reporting. Reference could also be made to ensure the data provider is aware of and follows their internal procedures for the handling and reporting of a data protection breach (if applicable).

Data Protection training

24. The Commissioner expects that a record of data protection training is kept, as this will be key in terms of demonstrating accountability under the GDPR. Under a revised strategy, reference could be made to this to advise participating bodies that a record of data protection training should be retained for accountability purposes. The same applies to the keeping of appropriate audit trails generally to evidence compliance.

Anonymisation and Pseudonymisation

25. The Commissioner seeks to ensure that the privacy rights of individuals are protected in relation to their personal data. However, in the Commissioner's view, the new data protection legislation should not be seen as a barrier to the open data agenda, but it does require a proper and rigorous risk assessment when datasets are derived from personal information.

26. It is the Commissioner's view that by assessing the risks properly and deploying techniques such as anonymisation and pseudonymisation in the right circumstances, organisations may be able to make information derived from personal data available in a form that is rich and usable, whilst protecting individual data subjects rights.

Pseudonymisation

27. As referred to in paragraph 14 of this response, pseudonymisation is a technique that is often used to help meet data protection obligations. Unlike anonymisation, pseudonymisation techniques will not exempt controllers from data protection responsibilities. Recital 26 of the GDPR makes it clear that pseudonymised personal data remains personal data and within the scope of the GDPR. "Personal data which have undergone pseudonymisation which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person."

28. Pseudonymisation may involve replacing names or other identifiers which are easily attributed to individuals with, for example, a reference number. Whilst you can tie that reference back to the individual if you have access to the relevant information, technical and organisational measures should be put in place to ensure that this information is held separately. Pseudonymising personal data

can reduce the risks to the data subjects and help an organisation meet its data protection obligations. However, as referred to in Recital 26 above, it is effectively only a security measure and does not change the status of the data as personal data. This must be borne in mind by data controllers who intend to provide data sets to the open data platform. Specific reference should be made to its unsuitability as a technique for rendering the data as open and truly unidentifiable. It should be noted that under Pt 6 Section 171 of the Data Protection Act 2018, it is a criminal offence to re-identify de-identified data without the consent of the data controller.

Anonymisation

29. As referred to in paragraph 13 of this response, anonymisation is a technique that can be used to render data suitable for inclusion in the drive for open data. When done properly anonymisation places the processing and storage of this data outside the scope of GDPR. It is no longer considered 'personal data' and the regulations do not therefore concern the processing of such anonymous information including for statistical or research purposes.

30. Anonymisation can therefore be a method of limiting your risk and a benefit to data subjects too. The anonymising of data wherever possible is therefore encouraged. However caution should be exercised when attempting to anonymise personal data. Organisations frequently refer to personal data sets as having been 'anonymised' when, in fact, this is not the case. Organisations must be confident that any treatments or approaches that are taken truly anonymise personal data.

31. The ICO's has guidance on Anonymisation in line with the GDPR. It also has a Code of Practice on Anonymisation which was produced for the old Data Protection Act 1998, but is still largely relevant. This Code will be updated in line with GDPR in the coming year. The code explains the process of converting personal data into a 'safe' anonymised form and stress the importance of assessing re – identification risk in particular circumstances. Providing data is anonymised to an acceptable standard, data protection legislation will not apply if the de-identification process has effectively anonymised the data.

DPIAs

32. Data Protection Impact Assessments form part of the 'data protection by design and default' and accountability approach under GDPR. Article 35 requires organisations to carry out a DPIA before carrying out types of processing that are likely to result in a high risk to the rights and freedoms of individuals in specified circumstances. It will be for the Department to decide whether the threshold of requiring a

DPIA is reached. Factors to be considered could be (but are not limited to) the scale of the processing that may be taking place, the use of technologies and approaches that a refreshed strategy may bring, and any data that may be used that has not been obtained directly from the data subject.

33. The Article 29 Working Party (now European Data Protection Board) published guidelines with nine criteria which may act as indicators of likely high risk processing. Under article 35(4) of the GDPR, the ICO has published a list of processing activities which may require a DPIA under certain circumstances. More information about these criteria can be found in our detailed guidance about DPIAs.

34. The ICO's Guidance on DPIAs states that even if there is no indication of likely high risk, it is good practice to do a DPIA for any major new project that may involve the use of personal data.

35. It would be beneficial for DoF to include information about DPIAs in its revised strategy. The Commissioner would also recommend that Departments publish any DPIA they may undertake on the open data work, their procedures for managing it and identifying any associated privacy risks that may be inherent in any associated processing operations.

36. Further information on DPIAs, including the obligation to consult the Commissioner in certain cases, is available here.

Freedom of Information Act 2000 and Open Data

37. The existing version of the Open Data Strategy made little reference to the Freedom of Information Act 2000 (FOIA). It's conclusion discussed the value that could be derived from the release of public sector data and reduction in administrative costs of answering FOI requests. Reference could be made to the existing provisions under FOIA for the release of information held by public authorities. The process of requesting information and public authorities responding to requests, considering any relevant exemptions and applying the public interest test where required, together with the right to complain to the Information Commissioner and to the Information Rights Tribunal, means that there already is in effect a continual assessment of what is possible to release and what should be withheld. In this way FOIA supports the open data agenda.

38. The Commissioner would note that the data which a public authority believes is beneficial to release is not necessarily the same as that which advocates of open data (and FOIA requesters) wish to obtain and re-use. The Commissioner believes that it is important to establish the types of information that public authorities should

routinely make available as open data. She believes that it is certainly beneficial to do this by engaging and in partnership with data users and intermediaries.

39. However, the right to request any other information is also an essential part of the open data agenda. Indeed this is supported by the data set provisions in FOIA which represent an obligation under section 19. These provisions cover how public authorities are required to make any dataset that has been requested from them available for re-use on an ongoing basis under their FOIA publication scheme (unless it is not appropriate to do so). This illustrates how the open data agenda and FOIA can be complementary. The Commissioner believes that it would be helpful for DoF to recognise the explicit link between the right of access and the right to re-use.

FOI Strategy and Outsourcing

40. Recent work by the Commissioner complements the objectives in the Open Data Strategy. She believes it is helpful to point out this work and that it should be considered during the refresh of the strategy.

41. The Commissioner recently set out her ambition to be more proactive and increase the impact of our regulation of access to information legislation.

42. The ICO is currently consulting on a draft access to information strategy. The new strategy entitled, 'Openness by Design. Our Draft access to information strategy' lays out the proposals for a three year programme of work for FOI and EIR. One of the key priorities proposed is to work in partnership to improve standards of openness, transparency and participation among public authorities in a digital age.

Outsourcing

43. The Commissioner has consistently supported open data and proactive measures to improve transparency. The Commissioner believes that democratic engagement and access to information law are also vital to this. On 28 January 2019, the ICO laid before Parliament a report about FOIA and EIR. The report, 'Outsourcing oversight? The case for reforming access to information law' focuses on the access to information laws set out in the FOIA and EIR. It also examines the impact that modern methods of delivering public services have on accountability and transparency, and sets out recommendations for change.

44. The ICO would welcome comments on the proposals set out in the draft strategy before 8 March 2019 to help inform a final version to be launched later in 2019. The Commissioner would encourage

engagement with the Belfast regional office of the ICO around the issues raised in this report and any implications this may have on the open data work in NI.

The Role of the Information Commissioner

45. In line with one of the priorities in her draft strategy as outlined in paragraph 42, the Commissioner has actively engaged with the Northern Ireland Civil Service on transparency, openness and good information governance and will continue this work over the forthcoming period. The Commissioner would welcome regional engagement with the DoF throughout the course of their Open Data Strategy consultation period and implementation phase. This includes the support of the Belfast regional office of the ICO in providing advice or assistance particularly in terms of the legislation we regulate which can complement the open data agenda.

46. It may also be helpful to add a link to the website of the Commissioner in the draft strategy as a point of reference.

47. Public bodies in Northern Ireland may contact the ICO's Northern Ireland Regional Office with any questions about data protection law or any other information rights law that we regulate. The contact details for our office are as follows:

    The Information Commissioner's Office
    3rd Floor
    14 Cromac Place
    Ormeau Road
    Belfast
    BT7 2JB

    Helpline: 0303 123 1113

    Email: ni@ico.org.uk

We trust these comments assist the Department in its review of strategy. The Commissioner would be happy to provide further information if requested.

Dr Ken Macdonald
Head of ICO Regions